Guiding Cyber Security through Collaboration

DOE 2012

Information Management Conference

Collaboration

- DOE Network Security Monitoring Group was formed out of a need for cyber security analysts to communicate and collaborate across the DOE Complex.
- Over the past 4 years we have been very successful in developing and sharing resources to enable cyber security analysts to respond to common threats.
- At the 2010 DOE Cyber Security Conference, NSM was awarded the Innovation in Collaboration Award.

History

- Began in May 2008 by a cyber security analyst who saw a need to share information among other analysts across the complex.
  - First meeting was hosted by JLAB
  - 24 people attended
- A pledge was created to remind everyone that we are fighting the same battles and only good can come from us working together.

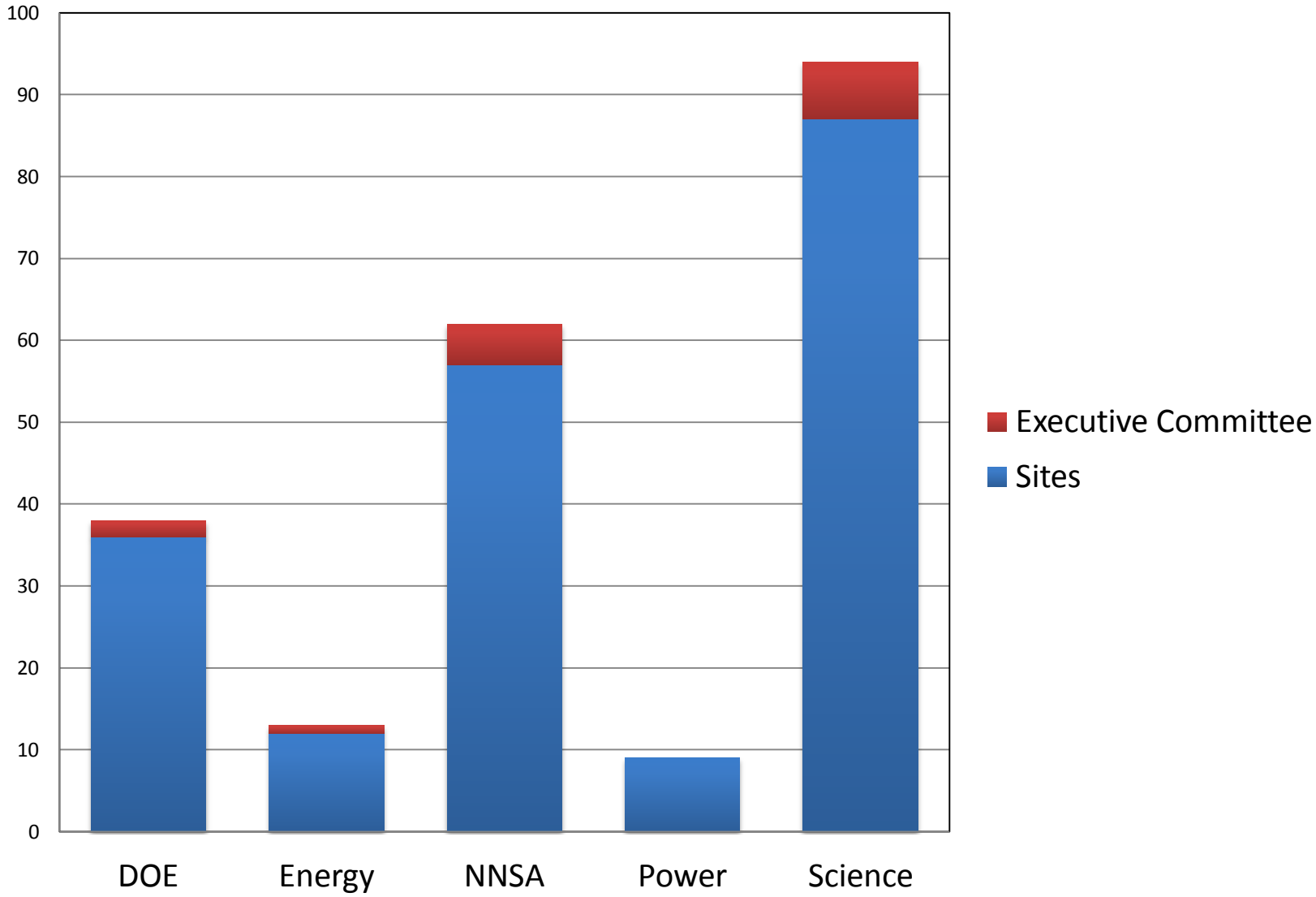
Newport News Pledge

- “Together we must work against our common threats. **A problem for me is a problem for everyone.** To address these threats I will collaborate freely and with integrity.”

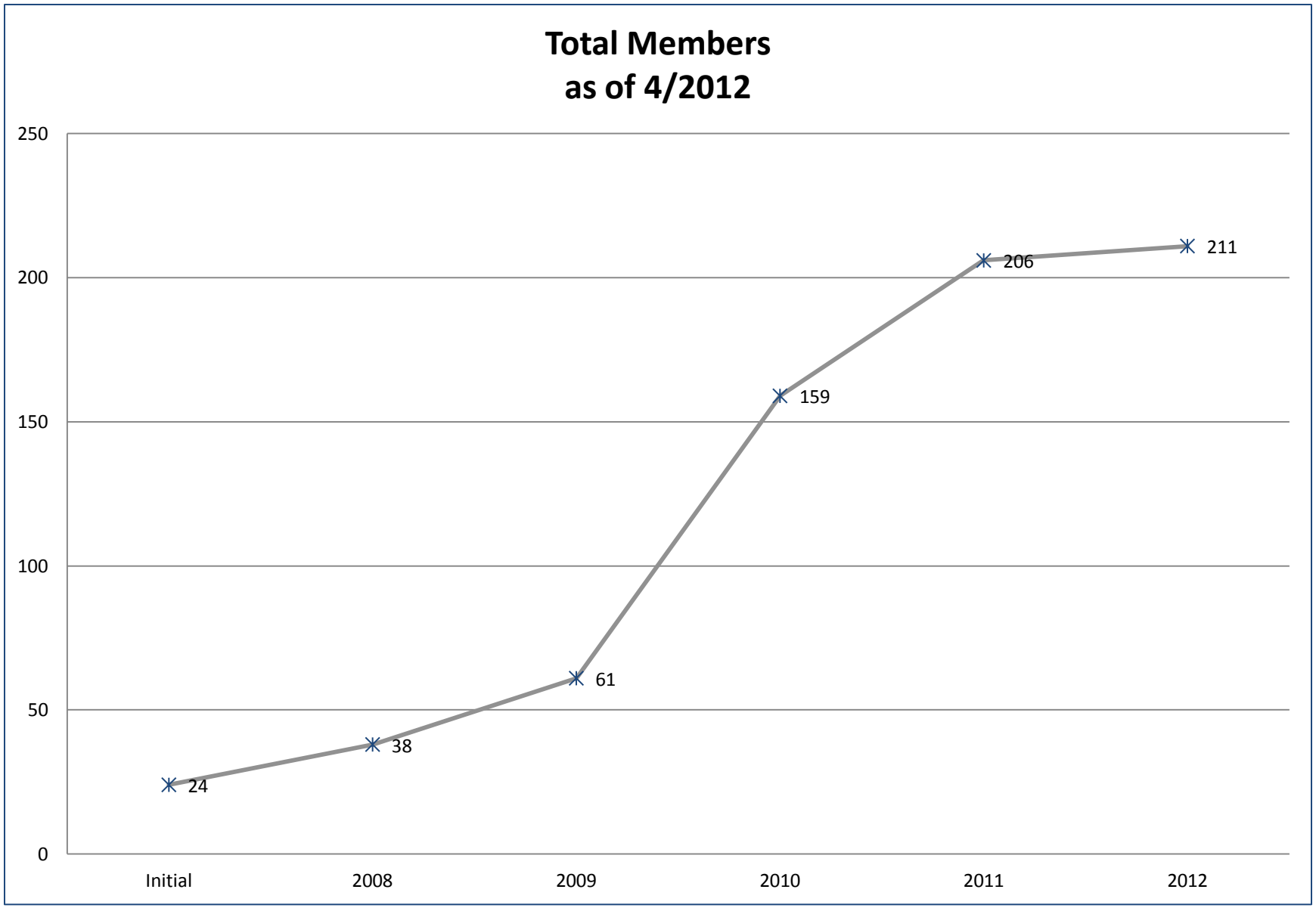
History

- Oct 2009 - Officially self-chartered (found on NSM Wiki)
- Executive Committee formed
- Membership requirements defined
- Focus of group is on operational cyber security.

NSM Membership



As of 3/2012


Total Members
as of 4/2012
250
200
150
100
50
0
24
38
61
159
206
211
Initial
2008
2009
2010
2011
2012

Membership

- The Network Security Monitoring group is comprised of cyber-analysts associated with the U.S. DOE Laboratories & Technology Centers, Offices and other DOE related entities (i.e. Power, Plants, etc). Members must be technical cyber security analysts or similar working for a DOE entity and approved by their sites' Cyber Security Program Manager.
- A volunteer executive community is elected yearly to plan for events, steward the resources, and manage the membership process

Group Resources

- NSM Summits (hosted by participating sites and the DOE Cyber Training Conference Committee)
  - Fall 2011 – Idaho National Laboratory
  - Fall 2012 – Sandia National Laboratory, Albuquerque
- Wiki (hosted by ANL)
- Forum site (hosted by ANL/operated by SNL)
- SILC Secure Chat (hosted by JC3)
- Encrypted and Clear Mailing Lists (hosted by JC3)
- GPG key chain
- Weekly Conference Call (hosted by JC3)
- Capability/SME Catalog
- Contact List

Activities and Accomplishments

- Training and awareness
  - Snort rule writing, OUO Threat Brief, Extraction from PCAPs, domain black holing, HSS Brief, rapid mal-ware analysis
  - IPv6 Security
- Allowed the community to get a feeling for the different sites' varied cyber competencies
- Fosters trust and identifies contact points for peer support in incident handling
- CPP, The Federated Model, JC3, and Tracer Fire have used the NSM group to find collaboration opportunities or participants
- Allowed collaborative real-time response across sites addressing a wide variety of cyber threats
- NSM Members participate and provide input to the DOE IPv6 Working Group.
- Provided input on Continuous Monitoring to the IMWG

Panel Discussion

- “facilitate outreach to members of the DOE security community with a vested interest in the DOE wide Sandbox …CTFO was also able to perform early testing and solicit additional ideas for features and enhancements …participation with NSM accelerated the development cycle of the DOE wide Sandbox effort. - Joshua Knust CTFO

- “leverage the technical peer-to-peer exchange of cyber security related information to support improving capabilities to proactively detect, react and respond to current and emerging threats.” – David Odom NNPP

Future

- Other Working Groups
  - AD Working Group
  - ???
- Collaboration has proven to be valuable in improving DOE's Cyber Security posture.